The Rabin cryptosystem revisitet

Elia, Michele ; Piva, Matteo ; Schipani, Davide

Abstract: The Rabin scheme used in public-key cryptosystem is here revisited with a focus limited to a few specific open issues. In particular, message decryption requires one out of four roots of a quadratic equation in a residue ring to be chosen, and a longstanding problem is to identify unambiguously and deterministically the encrypted message at the decryption side by adding the minimum number of extra bits to the cipher-text. While the question has already been solved for pairs of primes of the type $4k+3$, *the general problem is here addressed. As one of the major results, an explicit solution with two extra bits is provided for pairs a padding mechanism is proposed that avoids relying on a certain number of attempts until a suitable pad is found.*

DOI: https://doi.org/10.1007/s00200-014-0237-0

The Rabin cryptosystem revisited

Michele Elia[*], Matteo Piva [†], Davide Schipani [‡]

September 9, 2014

Abstract

The Rabin scheme used in public-key cryptosystem is here revisited with a focus limited to a few specific open issues. In particular, message decryption requires one out of four roots of a quadratic equation in a residue ring to be chosen, and a longstanding problem is to identify unambiguously and deterministically the encrypted message at the decryption side by adding the minimum number of extra bits to the cipher-text. While the question has already been solved for pairs of primes of the type $4k+3$, the general problem is here addressed. As one of the major results, an explicit solution with two extra bits is provided for pairs of primes that are congruent 5 modulo 8. The Rabin signature is also reconsidered from a deterministic point of view: a padding mechanism is proposed that avoids relying on a certain number of attempts until a suitable pad is found.

Keywords: Rabin cryptosystem, Jacobi symbols, Reciprocity, Residue Rings, Dedekind sums.

Mathematics Subject Classification (2010): 94A60, 11T71, 14G50

1 Introduction

In 1979, Michael Rabin [26] suggested a variant of RSA with public-key exponent 2, which he showed to be as secure as factoring. The encryption of a message $m \in \mathbb{Z}_N^*$ is $C = m^2 \bmod N$, where $N = pq$ is a product of two prime numbers, and decryption is performed by solving the equation

$$x^2 = C \bmod N \ , \tag{1}$$

which has four roots; thus for complete decryption, further information is needed to identify m among these roots. More precisely, for a fully automatic (deterministic) decryption, at least two more bits are needed (computed at the encryption stage) to identify m without ambiguity. The advantages of using this exponent 2, compared to larger exponents, are: i) a smaller computational burden, and ii) solving (1) is equivalent to factoring N. The disadvantages are: iii) computation, at the encryption stage, of the information required to identify the right root, and delivery of this

[*]Politecnico di Torino, Italy
[†]Universitá di Trento, Italy
[‡]University of Zurich, Switzerland

information to the decryption stage, and iv) vulnerability to chosen-plain-text attack [4, 21, 28, 15]. Several chosen methods base the selection of the correct root on the message semantics, that is they retain the root that corresponds to the message that looks most meaningful, or the root that contains a known string of bits. However, these methods are essentially probabilistic, and may affect the equivalence between breaking the Rabin scheme and factoring [4]. Nevertheless, for schemes using pairs of primes congruent 3 modulo 4 (Blum primes), Williams [31] proposed a root identification scheme based on the computation of a Jacobi symbol, using an additional parameter in the public key, and two additional bits in the encrypted message.
In 1988, Kurosawa et alii [18] proposed a function that is valid for every pair of primes, and possesses similar features to the Rabin scheme. Let a be a number of $\mathbb{Z}_N$, $N = pq$, such that

$$\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right) = -1$$

Kurosawa encryption of a message $m \in \mathbb{Z}_N$ is

$$E = m + \frac{a}{m}$$

with two extra bits computed as

$$t = \begin{cases} 0 & \text{if } \left(\frac{m}{N}\right) = 1 \\ 1 & \text{if } \left(\frac{m}{N}\right) = -1 \end{cases} \qquad s = \begin{cases} 0 & \text{if } \frac{a}{m} > m \\ 1 & \text{if } \frac{a}{m} < m \end{cases} .$$

Decryption entails solving the quadratic equation

$$X^2 - EX - a = 0$$

and choosing the root identified by the pair (t, s) [29]. This encryption algorithm is alternative to the Rabin algorithm, and works for every pair of primes. However, it must be noted that parameter a should be chosen appropriately, in order not to leak any information and expose the message to attacks, e.g. if a has small order k_p modulo p and large order modulo q, then $a^{k_p} - 1$ is divisible by p, i.e. $\gcd\{a^{k_p} - 1, N\} = p$.
In [19], this scheme is extensively considered and reformulated with a focus on semantic security, together with the RSA scheme and a modification of the Rabin algorithm, called Rabin-Paillier's algorithm, although the price to pay is to double the number of bits in the encrypted message. Semantic security, which is outside the scope of this paper, will not be examined in depth; however it will be shown how similar constructions can be adapted for this scheme with pairs of primes of the type $8k + 5$.
The Rabin cryptosystem may also be used to create a signature by exploiting inverse mapping: in order to sign m, the equation $x^2 = m \bmod N$ is solved and any of the four roots, say S, can be used to form the signed message (m, S). However, if $x^2 = m \bmod N$ has no solution, the signature cannot be directly generated; to overcome this, a random pad U can be used until $x^2 = mU \bmod N$ is solvable, and the signature is the triple (m, U, S) [25]. A verifier compares S^2 with $mU \bmod N$, and accepts the signature as valid when these two numbers are equal. For an application to electronic signature, an in-depth analysis of advantages and disadvantages can be found in [3].

The paper is organized as follows: Section 2 provides preliminary results concerning the solutions of equation (1) and the mathematics that will be needed. Section 3 describes in detail the Rabin scheme in the standard setting, where both prime factors of N are congruent 3 modulo 4, and proposes a new identification rule exploiting Dedekind sums. Section 4 addresses the identification problem for any pair of primes, featuring a deterministic scheme that works with primes congruent 5 modulo 8, based on quartic residues of Gaussian integers. A suboptimal solution that works for any pair of primes is also presented. Section 5 considers a Rabin signature with a new padding mechanism that avoids relying on attempts until a suitable pad is found. Forgery attacks are also examined, and countering strategies mentioned, in using this padding factor, although these questions are addressed more extensively in [8]. Lastly, Section 6 draws some conclusions.

2 Preliminaries

Let $N = pq$ be a product of two odd primes p and q. Using the generalized Euclidean algorithm to compute the greatest common divisor between p and q, two integer numbers, $\lambda_1, \lambda_2 \in \mathbb{Z}$, such that $\lambda_1 p + \lambda_2 q = 1$, are efficiently computed. Then, setting $\psi_1 = \lambda_2 q$ and $\psi_2 = \lambda_1 p$, so that $\psi_1 + \psi_2 = 1$, it is easily verified that ψ_1 and ψ_2 satisfy the relations

$$\begin{cases} \psi_1\psi_2 = 0 \bmod N \\ \psi_1^2 = \psi_1 \bmod N \\ \psi_2^2 = \psi_2 \bmod N \ . \end{cases} \tag{2}$$

and that $\psi_1 = 1 \bmod p$, $\psi_1 = 0 \bmod q$, and $\psi_2 = 0 \bmod p$, $\psi_2 = 1 \bmod q$. According to the Chinese Remainder Theorem (CRT), using ψ_1 and ψ_2, every element a in $\mathbb{Z}_N$ can be represented as

$$a = a_1\psi_1 + a_2\psi_2 \bmod N \ ,$$

where $a_1 \in \mathbb{Z}_p$ and $a_2 \in \mathbb{Z}_q$ are calculated as $a_1 = a \mod p$, $a_2 = a \mod q$.
The four roots $x_1, x_2, x_3, x_4 \in \mathbb{Z}_N$ of (1), represented as positive numbers, are obtained using the CRT from the roots $u_1, u_2 \in \mathbb{Z}_p$ and $v_1, v_2 \in \mathbb{Z}_q$, of the two equations $u^2 = C \mod p$ and $v^2 = C \mod q$, respectively. The roots u_1 and $u_2 = p - u_1$ are of different parities; likewise, v_1 and $v_2 = q - v_1$. If p is congruent 3 modulo 4, the root u_1 can be computed in deterministic polynomial-time as $\pm C^{\frac{p+1}{4}} \bmod p$; the same holds for q. If p is congruent 1 modulo 4, an equally simple algorithm is not known; however, u_1 can be computed in probabilistic polynomial-time using Tonelli's algorithm [2, 21] once a quadratic non-residue modulo p is known (this computation is the probabilistic part of the algorithm), or using the (probabilistic) Cantor-Zassenhaus algorithm [5, 9, 30] to factor the polynomial $u^2 - C$ modulo p. Using the previous notations, the four roots of (1) can be written as

$$\begin{cases} x_1 = u_1\psi_1 + v_1\psi_2 & \bmod N \\ x_2 = u_1\psi_1 + v_2\psi_2 & \bmod N \\ x_3 = u_2\psi_1 + v_1\psi_2 & \bmod N \\ x_4 = u_2\psi_1 + v_2\psi_2 & \bmod N \ . \end{cases} \tag{3}$$

Lemma 1 *Let $N = pq$ be a product of two prime numbers. Let C be a quadratic residue modulo N; the four roots x_1, x_2, x_3, x_4 of the polynomial $x^2 - C$ are partitioned into two sets $\mathfrak{X}_1 = \{x_1, x_4\}$ and $\mathfrak{X}_2 = \{x_2, x_3\}$ such that roots in the same set have different parities, i.e. $x_1 = 1 + x_4 \bmod 2$ and $x_2 = 1 + x_3 \bmod 2$.*

Furthermore, assuming that u_1 and v_1 in equation (3) have the same parity, the residues modulo p and modulo q of each root in $\mathfrak{X}_1$ have the same parity, while each root in $\mathfrak{X}_2$ has residues of different parities.

PROOF. Since u_1 and v_1 have the same parity by assumption, then also u_2 and v_2 have the same parity. The connection between x_1 and x_4 is shown by the following chain of equalities

$$x_4 = u_2\psi_1 + v_2\psi_2 = (p - u_1)\psi_1 + (q - v_1)\psi_2 = -x_1 \bmod N = N - x_1 \ ,$$

because $p\psi_1 = 0 \bmod N$ and $q\psi_2 = 0 \bmod N$, and x_1 is less than N by assumption, thus $-x_1 \bmod N = N - x_1$ is positive and less than N. A similar chain connects x_2 and $x_3 = N - x_2$; the conclusion follows because N is odd and thus x_1 and x_4, as well as x_2 and x_3, have different parities.

□

2.1 The Mapping $\mathfrak{R}: \ x \to x^2$

The mapping $\mathfrak{R}: \ x \to x^2$ is four-to-one and partitions $\mathbb{Z}_N^*$ into disjoint subsets $\mathfrak{u}$ of four elements specified by equation (3). Let $\mathfrak{U}$ be the group of the four square roots of unity, that is the roots of $x^2 - 1$ consisting of the four-tuple

$$\mathfrak{U} = \{1, \psi, -\psi, -1\} \ ,$$

where

$$\psi = \psi_1 - \psi_2 \bmod N \ . \tag{4}$$

Obviously, $\mathfrak{U}$ is a group of order 4 and exponent 2. Each subset $\mathfrak{u}$, consisting of the four square roots of a given quadratic residue, may be described as a coset $m\mathfrak{U}$ of $\mathfrak{U}$, i.e.

$$\mathfrak{u} = m\mathfrak{U} = \{m, \psi m, -\psi m, -m\} \ .$$

The number of these cosets is $\frac{\phi(N)}{4}$, and they form a group which is isomorphic to a subgroup of $\mathbb{Z}_N^*$ of order $\phi(N)/4$. Once a coset $\mathfrak{u} = \{x_1, x_2, x_3, x_4\}$ is given, the problem is to identify the four elements contained in it. By Lemma 1, each x_i is identified by the pair of bits

$$b_p = (x_i \bmod p) \bmod 2, \ \text{ and } \ b_q = (x_i \bmod q) \bmod 2 \ .$$

In summary, the table

root	b_p	b_q
x_1	$u_1 \bmod 2$	$v_1 \bmod 2$
x_2	$u_1 \bmod 2$	$v_2 \bmod 2$
x_3	$u_2 \bmod 2$	$v_1 \bmod 2$
x_4	$u_2 \bmod 2$	$v_2 \bmod 2$

shows that two bits identify each of the four roots. On the other hand, the expression of these two bits involves the prime factorization of N, that is p and q, but when the factors of N are not available, it is no longer possible to compute these parity bits, and the problem is to find which parameters can be used, and the minimum number of additional bits that must be disclosed in

order to label a given root among the four.
Adopting the convention introduced along with equation (3), a parity bit, namely $b_0 \doteq x_i \bmod 2$, distinguishes x_1 from x_4, and x_2 from x_3, therefore it may be one of the parameters to be used in identifying the four roots. It remains to determine how to distinguish between roots having the same parity, without knowing the factors of N.

2.2 Dedekind sums

A Dedekind sum is denoted by $s(h,k)$ and defined as follows [27]. Let h,k be relatively prime and $k \geq 1$, then we set

$$s(h,k) = \sum_{j=1}^{k} \left(\left(\frac{hj}{k} \right) \right) \left(\left(\frac{j}{k} \right) \right) \tag{5}$$

where the symbol $((x))$, defined as

$$((x)) = \begin{cases} x - \lfloor x \rfloor - \frac{1}{2} & \text{if } x \text{ is not an integer} \\ 0 & \text{if } x \text{ is an integer} \end{cases}, \tag{6}$$

denotes the well-known sawtooth function of period 1. The Dedekind sum satisfies the following properties, see [6, 13, 27] for proofs and details:

1) $h_1 = h_2 \bmod k \Rightarrow s(h_1,k) = s(h_2,k)$
2) $s(-h,k) = -s(h,k)$
3) $s(h,k) + s(k,h) = -\frac{1}{4} + \frac{1}{12}\left(\frac{h}{k} + \frac{1}{hk} + \frac{k}{h}\right)$, a property known as the reciprocity theorem for Dedekind sums.
4) $12ks(h,k) = k + 1 - 2\left(\frac{h}{k}\right) \bmod 8$ for k odd, a property connecting Dedekind sums and Jacobi symbols.

The first three properties make it possible to compute a Dedekind sum by a method that mimics the Euclidean algorithm and has the same efficiency. In the sequel the following Lemma is needed:

Lemma 2 *If $k = 1 \bmod 4$, then, for any h relatively prime with k, the denominator of $s(h,k)$ is odd.*

PROOF. In the definition of $s(h,k)$ the summation can be limited to $k-1$, because $\left(\left(\frac{k}{k} \right) \right) = 0$, furthermore, from the identity $((-x)) = -((x))$ it follows that $\sum_{j=1}^{k-1} \left(\left(\frac{hj}{k} \right) \right) = 0$ for every integer h [27]. We may thus write

$$s(h,k) = \sum_{j=1}^{k-1} \left(\frac{j}{k} - \frac{1}{2} \right) \left(\frac{hj}{k} - \left\lfloor \frac{hj}{k} \right\rfloor - \frac{1}{2} \right) = \sum_{j=1}^{k-1} \frac{j}{k} \left(\frac{hj}{k} - \left\lfloor \frac{hj}{k} \right\rfloor - \frac{1}{2} \right) ,$$

since $\left(\left(\frac{hj}{k} \right) \right)$ is never 0, because $j < k$ and h is relatively prime with k by hypothesis. The last summation can be split into the sum of two further summations, such that

- the first summation $\sum_{j=1}^{k-1} \frac{j}{k}\left(\frac{hj}{k} - \left\lfloor \frac{hj}{k} \right\rfloor\right)$ has the denominator patently odd;

- the second summation is evaluated as $-\frac{1}{2}\sum_{j=1}^{k-1} \frac{j}{k} = -\frac{k-1}{4}$.

In conclusion, the denominator of $s(h,k)$ is odd because $s(h,k)$ is the sum of a fraction with odd denominator with $-\frac{k-1}{4}$, which is an integer number by hypothesis.

□

3 The Rabin scheme: primes $p \equiv q \equiv 3 \bmod 4$

As said in the introduction, an important issue in using the Rabin scheme is to select the right root at the decryption stage. If $p \equiv q \equiv 3 \bmod 4$, a solution to the identification problem has been proposed by Williams [31] and is reported below, slightly modified from [25], along with three different solutions, including a new method based on Dedekind sums.

3.1 Variant I

A simpler variant [12] exploiting the Jacobi symbol is the following:

Public-key: $[N]$.

Encrypted message $[C, b_0, b_1]$, where

$$C = m^2 \bmod N \quad , \quad b_0 = m \bmod 2 \quad \text{and} \quad b_1 = \frac{1}{2}\left[1 + \left(\frac{m}{N}\right)\right] \ .$$

Decryption stage :

- compute, as in (3), the four roots, written as positive numbers,
- take the two roots having the same parity specified by b_0, say z_1 and z_2,
- compute the numbers

$$\frac{1}{2}\left[1 + \left(\frac{z_1}{N}\right)\right] \qquad \frac{1}{2}\left[1 + \left(\frac{z_2}{N}\right)\right]$$

and take the root corresponding to the number equal to b_1.

Remark 1. The two additional bits are sufficient to uniquely identify m among the four roots, because, as previously observed in Lemma 1, the roots have the same parity in pairs, and within each of these pairs the roots have opposite Jacobi symbols modulo N. In fact, roots with the same parity are of the form $a_1\psi_1 + a_2\psi_2$ and $a_1\psi_1 - a_2\psi_2$ (or $-a_1\psi_1 + a_2\psi_2$), whence the conclusion follows from

$$\left(\frac{a}{N}\right) = \left(\frac{a_1\psi_1 + a_2\psi_2}{pq}\right) = \left(\frac{a_1\psi_1 + a_2\psi_2}{p}\right)\left(\frac{a_1\psi_1 + a_2\psi_2}{q}\right) = \left(\frac{a_1}{p}\right)\left(\frac{a_2}{q}\right) \qquad (7)$$

and the fact that -1 is a nonresidue modulo a Blum prime.

3.2 Variant II

There is a second variant exploiting the Jacobi symbol which, at some extra computational cost and with some further information in the public key, requires the delivery of no further bit, since the information needed to decrypt it is carried by the encrypted message itself [12, 10]. An adapted version is the following. Let ξ be an integer such that $\left(\frac{\xi}{p}\right) = -\left(\frac{\xi}{q}\right) = 1$, for example $\xi = \alpha^2\psi_1 - \psi_2 \bmod N$, with $\alpha \in \mathbb{Z}_N^*$. The detailed process consists of the following steps

Public-key: $[N, \xi]$.

Encrypted message $[C]$, where C is obtained as follows

$$C' = m^2 \bmod N \ , \ b_0 = m \bmod 2 \ , \ b_1 = \frac{1}{2}\left[1 - \left(\frac{m}{N}\right)\right] \quad \text{and} \quad C = C'(-1)^{b_1}\xi^{b_0} \bmod N \, .$$

Decryption stage :

- compute $d_1 = \frac{1}{2}\left[1 - \left(\frac{C}{p}\right)\right]$, and set $C" = C(-1)^{d_1}$
- compute $d_0 = \frac{1}{2}\left[1 - \left(\frac{C}{N}\right)\right]$, and set $\hat{C} = C"\xi^{-d_0}$
- compute, as in (3), the four roots of $\hat{C}$, written as positive numbers.
- take the root identified by b_0 and b_1

Decryption works, since we have $\hat{C} = C(-1)^{d_1}\xi^{-d_0} = C'(-1)^{b_1}\xi^{b_0}(-1)^{d_1}\xi^{-d_0} = C'$, due to the coincidences $d_0 = b_0$ and $d_1 = b_1$. Indeed, the following two chains of equalities, which are a consequence of the definition of ξ, the fact that C' is a quadratic residue modulo N, and lastly that (-1) is a quadratic non-residue modulo p and q

$$\left(\frac{C}{N}\right) = \left(\frac{C'}{N}\right)\left(\frac{(-1)^{b_1}}{N}\right)\left(\frac{\xi^{b_0}}{N}\right) = \left(\frac{\xi^{b_0}}{p}\right)\left(\frac{\xi^{b_0}}{q}\right) = \left(\frac{\xi^{b_0}}{q}\right) = (-1)^{b_0}$$

$$\left(\frac{C}{p}\right) = \left(\frac{C'}{p}\right)\left(\frac{(-1)^{b_1}}{p}\right)\left(\frac{\xi^{b_0}}{p}\right) = \left(\frac{(-1)^{b_1}}{p}\right) = (-1)^{b_1} \ ,$$

afford the final identification of d_0 and d_1 with b_0 and b_1, respectively.

Remark 2. Note that the Jacobi symbol $\left(\frac{C}{N}\right)$ discloses the message parity to an eavesdropper.

3.3 Williams' scheme

Williams [25, 31] first proposed an implementation of the Rabin cryptosystem, using a parity bit and the Jacobi symbol, but adding an additional parameter in the public key.

The decryption process is based on the observation that, setting $D = \frac{1}{2}(\frac{(p-1)(q-1)}{4} + 1)$, if $b = a^2 \bmod N$ and $\left(\frac{a}{N}\right) = 1$, so that $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right)$, we have $b^D = a\left(\frac{a}{p}\right) = a\left(\frac{a}{q}\right)$, given that

$$a^{\frac{\varphi(N)}{4}} = (a\psi_1 + a\psi_2)^{\frac{\varphi(N)}{4}} = a^{\frac{\varphi(N)}{4}}\psi_1 + a^{\frac{\varphi(N)}{4}}\psi_2 = \left(\frac{a}{p}\right)\psi_1 + \left(\frac{a}{q}\right)\psi_2 = \left(\frac{a}{p}\right) = \left(\frac{a}{q}\right) \bmod N,$$

as $a^{\frac{p-1}{2}} = \left(\frac{a}{p}\right) \bmod p$, $a^{\frac{q-1}{2}} = \left(\frac{a}{q}\right) \bmod q$, $\frac{p-1}{2}$ and $\frac{q-1}{2}$ are odd (cf. also Lemma 1 in [31]), and $\psi_1 + \psi_2 = 1$.

Public-key: $[N, S]$, where S is an integer such that $\left(\frac{S}{N}\right) = -1$.

Encrypted message $[C, c_1, c_2]$, where

$$c_1 = \frac{1}{2}\left[1 - \left(\frac{m}{N}\right)\right] \quad , \quad \bar{m} = S^{c_1} m \bmod N \quad , \quad c_2 = \bar{m} \bmod 2 \quad , \text{ and } \quad C = \bar{m}^2 \bmod N \ .$$

Decryption stage :

compute $m' = C^D \bmod N$ and $N - m'$, and choose the number, m'' say, with the parity specified by c_2. The original message is recovered as

$$m = S^{-c_1} m'' \bmod N \ .$$

3.4 A scheme based on Dedekind sums

Let $m \in \mathbb{Z}_N$ be the message to be encrypted, with $N = pq$, $p \equiv q \equiv 3 \bmod 4$. The detailed process consists of the following steps:

Public-key: $[N]$.

Encrypted message $[C, b_0, b_1]$, where

$$C = m^2 \bmod N \quad , \quad b_0 = m \bmod 2 \quad , \text{ and } \quad b_1 = s(m, N) \bmod 2 \ ,$$

in which, due to Lemma 2, the Dedekind sum can be taken modulo 2 since the denominator is odd.

Decryption stage :

- compute, as in (3), the four roots, written as positive numbers,
- take the two roots having the same parity specified by b_0, say z_1 and z_2,
- compute the numbers

$$s(z_1, N) \bmod 2 \qquad s(z_2, N) \bmod 2 \ ,$$

and take the root corresponding to the number equal to b_1.

The algorithm works because $s(z_1, N) \bmod 2 \neq s(z_2, N) \bmod 2$ by the following Lemma.

Lemma 3 *If k is the product of two Blum primes p and q, $(x_1, k) = 1$, and $x_2 = x_1(\psi_1 - \psi_2)$, then*

$$s(x_1, k) + s(x_2, k) = 1 \bmod 2 \ .$$

PROOF.
By property 4) in Section 2.2, which compares the value of the Dedekind sum with the value of the Jacobi symbol, we have

$$12Ns(x_1, N) = N + 1 - 2\left(\frac{x_1}{N}\right) \bmod 8 \quad \text{and} \quad 12Ns(x_2, N) = N + 1 - 2\left(\frac{x_2}{N}\right) \bmod 8;$$

summing the two expressions (member by member) and taking into account that $N = 1 \bmod 4$ we have

$$12N(s(x_1, N) + s(x_2, N)) = 2N + 2 - 2\left[\left(\frac{x_1}{N}\right) + \left(\frac{x_2}{N}\right)\right] \bmod 8\ ,$$

since $12N = 4 \bmod 8$, $2N = 2 \bmod 8$. Now, it was shown above (cf. Remark 1) that the sum of the two Jacobi symbols is 0; then, applying Lemma 2, we have

$$4(s(x_1, N) + s(x_2, N)) = 4 \bmod 8 \ \Rightarrow \ s(x_1, N) + s(x_2, N) = 1 \bmod 2\ ,$$

which concludes the proof.

□

4 Root identification for any pair of primes

If p and q are not both Blum primes, identification of m among the four roots of the equation $x^2 - C$, where $C = m^2 \bmod N$, can be given by the pair $[b_0, b_1]$ where

$$b_0 = x_i \bmod 2 \quad \text{and} \quad b_1 = (x_i \bmod p) + (x_i \bmod q) \bmod 2\ ,$$

as a consequence of Lemma 1. The bit b_0 can be computed at the encryption stage without knowing p nor q, while b_1 requires, in this definition, p and q to be known, and cannot be directly computed knowing only N.
In principle, a way to obtain b_1 is to publish a pre-computed binary list (or table) that has, in position i, the bit b_1 pertaining to the message $m = i$. This list does not disclose any useful information on the factorization of N because, even if we know that the residues modulo p and modulo q have the same parity, we do not know which parity, and if these residues have different parities we do not know which is which. Although the list makes the task theoretically feasible, its size is of exponential complexity with respect to N, and thus practically unrealizable.
When N is a product of two Blum primes, the second bit b_1 can be computed using the Jacobi symbol, as seen in Section 3, where b_1 is obtained by exploiting properties of the quadratic residuosity. However, for primes congruent 1 modulo 4, quadratic residuosity cannot distinguish numbers of opposite signs and is no longer sufficient to identify the roots. Higher power residue symbols could in principle do the desired job, but unfortunately their use is not straightforward, and analogous reciprocity laws or multiplicative properties are not always at hand.
Higher power residues have, indeed, been used in some generalizations of the Rabin scheme, working in residue rings modulo non-prime ideals of algebraic number fields. For instance, residue rings in Eisenstein or Gauss fields were considered in [29], which introduced Rabin-like schemes based on encryption rules involving powers of the message higher than 2. However,

this approach does not address the problem of separating the roots of a quadratic equation in the original Rabin scheme.
Before presenting a neat solution of this root identification problem, using quartic reciprocity for primes congruent 5 modulo 8, the difficulties and some attempts concerning a general solution for non-Blum primes will be examined.
Let 2^k and 2^h be the even exponents of $\mathbb{Z}_p$ and $\mathbb{Z}_q$, respectively, that is 2^k strictly divides $(p-1)$ and 2^h strictly divides $(q-1)$, and assume that $k \geq h$. The rational power residue symbols $x^{\frac{p-1}{2^k}} \bmod p$ and $x^{\frac{q-1}{2^h}} \bmod q$ can then, respectively, distinguish between u_1 and u_2, and between v_1 and v_2. Since it is desire to use N as a modulo, the idea of multiplying the exponents and considering the function $x^{\frac{\phi(N)}{2^{k+h}}} \bmod N$, which would identify m among the 2^{k+h} 2^k-th roots of unity in $\mathbb{Z}_N^*$, is examined. The idea would be to make these roots publicly available and label them, so that the sender of the message can tell which of them corresponds to the message actually sent. There are two problems with this: first, the exponent $\frac{\phi(N)}{2^{k+h}}$ should also be available, but necessarily in some masked form via multiplication by an odd number, in order to hide the factors of N; but, most importantly, among the public 2^k-th roots of unity we would find the square roots, and in particular $K \doteq \psi_1 - \psi_2$. However, the greatest common divisor of $K+1 = 2\psi_1$ and N yields q, and so N would be factored.
The idea will now be clarified by examining this point in greater depth. The multiplicative group $\mathbb{Z}_N^*$, the direct product of two cyclic groups $\mathfrak{C}_{p-1}$ and $\mathfrak{C}_{q-1}$, can also be viewed as the direct product of two abelian subgroups, namely a 2-group and a group of odd order, that is

$$\mathbb{Z}_N^* = (\mathfrak{C}_{2^k} \times \mathfrak{C}_{2^h}) \times \left(\mathfrak{C}_{2f_p+1} \times \mathfrak{C}_{2f_q+1}\right) \ .$$

Therefore, every element a of $\mathbb{Z}_N^*$ can be written as a product $a_2 a_o$ where a_o is an element of odd order, and a_2 is an element of order a power of 2, i.e. it is an element of a 2-group which has rank 2 and exponent 2^k.
The four roots $\mathbf{V}_4 = \{1, -1, \psi, -\psi\}$ of 1, where $\psi = \psi_1 - \psi_2 \bmod N$, form a group of order 4 (the Vierergruppe) of rank 2, and generators -1 and ψ. Let a be a quadratic residue, then its four square roots $\{A, A_1, A_2, A_3\}$ may be written as $\{A, -A, A\psi, -A\psi\}$, choosing now to consider remainders modulo N of absolute value less than $N/2$.
A specific square root m of a among $\{A, -A, A\psi, -A\psi\}$ is identified by the sign of m and a further number c, possibly a single bit, which should be computed with the constraint of using N, m, and some additional public information that should not disclose the factors p and q of N. Leaving aside this last constraint for the moment, it will be shown how to compute c using a sort of residuosity of convenient order depending on the group $\mathfrak{C}_{2^k} \times \mathfrak{C}_{2^h}$.
Let $2f_N + 1 = \text{lcm}\{2f_p + 1, 2f_q + 1\}$ be the maximum order of the elements in the subgroup of odd order, therefore $a_o^{2f_N+1} = 1 \bmod N$. Since $2f_N + 1$ and 2^k are relatively prime, then a generalized Euclidean algorithm gives α and β such that $\alpha(2f_N + 1) + \beta 2^k = 1$, then we have

$$m^{\alpha(2f_N+1)} = (m_2 m_o)^{\alpha(2f_N+1)} = m_2^{\alpha(2f_N+1)} m_o^{\alpha(2f_N+1)} = m_2^{\alpha(2f_N+1)} = m_2^{1-\beta 2^k} = m_2 \bmod N \ .$$

Therefore, an exponentiation with exponent $\alpha(2f_N + 1)$ defines an homomorphism θ of the group $\mathbb{Z}_N^*$ onto the subgroup $\mathcal{G}_2 = \mathfrak{C}_{2^k} \times \mathfrak{C}_{2^h}$, such that four-tuples $\mathbf{w}_b$ of square roots of the same element b in $\mathbb{Z}_N^*$ are mapped into four-tuples $\mathbf{g}_{\theta(b)}$ of square roots of the same element $\theta(b)$ in $\mathcal{G}_2$. Therefore, in order to identify any specified four-tuple of roots, it is sufficient to consider its image in $\mathcal{G}_2^4$. It

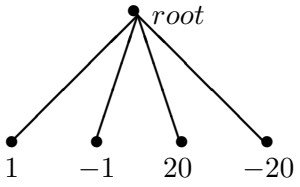

Figure 1: Tree representation of the 2-group of order 2×2 in $\mathbb{Z}^*_{7\cdot 19}$

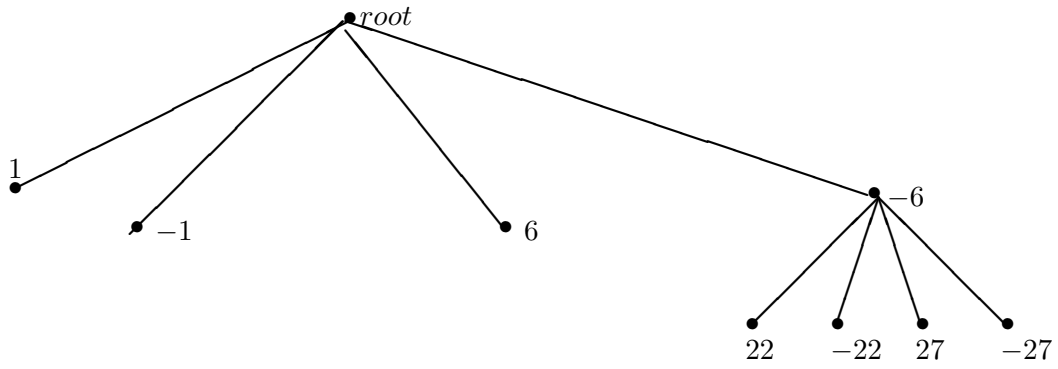

Figure 2: Tree representation of the 2-group of order $2^2 \times 2$ in $\mathbb{Z}^*_{5\cdot 7}$

is then useful to consider the partition of $\mathcal{G}_2$ into 4-tuples that are cosets of the group $\mathbf{V}_4$ of the square roots of 1.
The situation can be described pictorially using a 4-ary rooted tree $\mathfrak{T}$ with nodes labeled by the elements of the 2-group $\mathcal{G}_2$. The four nodes in the first layer below the root are labeled by the four roots of unity. In this layer, the node labeled with 1 is a terminal node; the remaining three nodes may or may not be terminal nodes depending on the form of the primes p and q. The height of the tree is $k(\geq h)$; the number of nodes in each level is a multiple of 4, and depends on the forms of the primes p and q. If there is a path (a sequence of branches) connecting a node u with a node v of a higher layer, v is said to be above u.
As an example, Figures 1, 2, and 3 show every possible shape of trees with at most two layers. In particular, the tree in Figure 1 corresponds to a pair of primes congruent 3 modulo 4; the tree in Figure 2 corresponds to a pair of primes, one congruent 3 modulo 4 and the second congruent 5 modulo 8; lastly, the tree in Figure 3 corresponds to a pair of primes congruent 5 modulo 8.
Note that every set of four nodes, directly connected to the same node, can be identified by a single label, say the coset leader, since the set of labels of these nodes can be seen as a coset of $\mathbf{V}_4$.
The next two lemmas show how to use the tree to identify the correct root of $X^2 = b \bmod N$, but, unfortunately, they also show that the residuosity connected with $\theta(.)$ discloses the factorization of N.

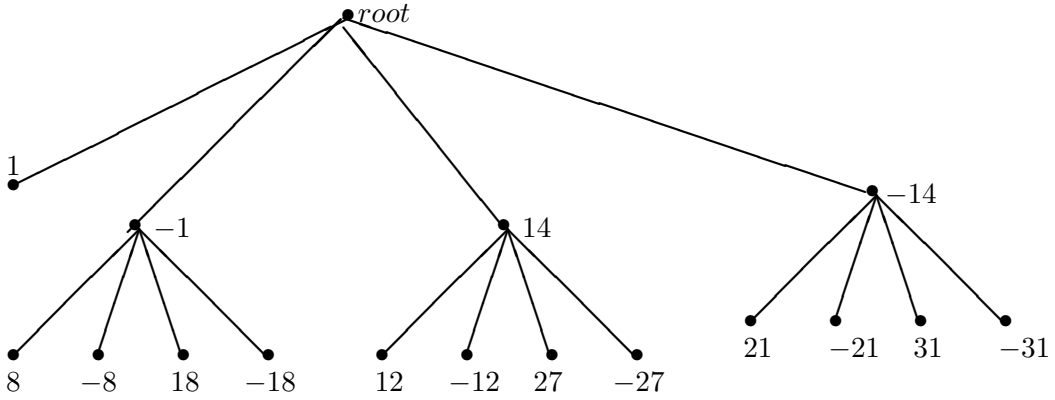

Figure 3: Tree representation of the 2-group of order $2^2 \times 2^2$ in $\mathbb{Z}^*_{5\cdot 13}$

Lemma 4 *Assume that the exponent $\alpha(2f_N + 1)$ is public, together with a table T of 2^{h+k-2} elements, containing one of the two positive elements for each set of 4 elements of the group $\mathcal{G}_2$, as described in its tree representation. Then, only two bits are sufficient to identify a square root m of b, that is, one bit for the sign of m, and one bit telling whether $|\theta(m)|$, the absolute value of $\theta(m)$, can or cannot be found in the table.*

PROOF When the sender wants to encrypt m, then the triple $\{b, b_0, b_1\}$ is sent, where $b = m^2 \bmod N$, b_0 is the sign of m, and $b_1 = \mathfrak{I}(|\theta(m)| \in T)$, with $\mathfrak{I}$ being the indicator function.
Given $[b, b_0, b_1]$ and knowing the factorization of $N = pq$, the right value m is identified as follows:

1. Solve the equation $x^2 = b \bmod N$ and find four values $[A, -A, B, -B]$
2. Compute $[|\theta(A)|, |\theta(B)|]$, one of these two values is in the table, therefore select the one compatible with b_1.
3. Define the correct value m using the previous value and b_0.

□

Unfortunately, the disclosure of $\alpha(2f_N + 1)$ leads to factoring N.

Lemma 5 *Assuming that $\alpha(2f_N + 1)$ is known, then the probability of factoring N is not less than $1/2$.*

PROOF It has been shown that, knowing ψ, N can be factored. Picking an integer x_r at random, the probability that $u = x_r^{\alpha(2f_N+1)}$ is below ψ or $-\psi$ in the tree is at least $1/2$. In the favorable event that u is below ψ or $-\psi$, a power of u with a convenient exponent $2^{f(u)}$ gives ψ. The probability is exactly $1/2$ in the case of Blum primes, otherwise it is greater, as can be deduced from the trees.

□

In conclusion, the scheme allows us in principle to compute two bits discriminating the four roots of b, by means of functions computable using only m, N and not its factorization. Unfortunately, the additional information made public, the table and the exponent, permit the factorization of

N deterministically, since ψ can be retrieved from the table, as well as probabilistically with high probability, as a consequence of Lemma 5.
Therefore, it is necessary to look at different kinds of higher-order residuosity, which should provide

- a definition of symbols a la Jacobi specifying the residue character;
- a reciprocity law for these symbols;
- the values of the symbols should belong to a finite group which does not reveal any information allowing the factorization of N.

Let ℓ denote the height of the tree $\mathfrak{T}$, and ζ_{2^ℓ} be a primitive root of unity; it turns out that such a 2^ℓ-residuosity exists in the ring of integers $\mathbb{Z}[\zeta_{2^\ell}]$ of cyclotomic fields $\mathbb{Q}(\zeta_{2^\ell})$. Let $\nu \in \mathbb{Z}[\zeta_{2^\ell}]$ be irreducible. A symbol of residuosity may be defined, [11, Theorem 46, p.211], as

$$\left[\frac{b}{\nu}\right]_{2^\ell} = b^{\frac{\mathcal{N}(\nu)-1}{2^\ell}} \bmod \nu = \zeta_{2^\ell}^{\gamma(b)}, \tag{8}$$

where $\mathcal{N}(\nu)$ is the norm of ν in $\mathbb{Q}(\zeta_{2^\ell})$, $\gamma(b)$ is an integer that certainly exists, since ζ_{2^ℓ} and $b^{\frac{\mathcal{N}(\nu)-1}{2^\ell}}$ are both roots of $X^{2^\ell} - 1 \bmod \nu$.
Using this residuosity, the difficulty becomes that of computing $\gamma(b)$; however, in the case of quartic residuosity, the task is made possible by Gauss-Jacobi's quartic residue symbols and their reciprocity law, as will be shown in the next subsection.

4.1 Identification scheme using quartic residuosity

Assuming that p and q are congruent 5 modulo 8, it will now be shown that the quartic residuosity in Gaussian integers is sufficient to discriminate the 4 square roots with exactly 2 bits.
Let $\mathbb{Z}[i]$ be the ring of Gaussian integers, which is Euclidean, so that the factorization is unique except for a reordering and a multiplication by units. The units are $\mathfrak{U} = \{1, -1, i, -i\}$ and form a cyclic group [14]. Any integer $z = x + iy$ in $\mathbb{Z}[i]$ has four associates, namely $z, -z, iz$, and $-iz$. In $\mathbb{Z}[i]$ the rational primes p congruent 1 modulo 4 split as $p = (a + ib)(a - ib)$, and 2 splits as $2 = (1 + i)(1 - i)$. The following notions and properties are taken from [16, p.119-127], which we refer to for proofs and details.

Definition 1 *An integer $x + iy$ of $\mathbb{Z}[i]$ is said to be* primary *if $x + iy = 1 \bmod (1 + i)^3$.*
An integer $z \in \mathbb{Z}[i]$ is said to be odd if it is not divisible by $1 + i$.
The norm of $x + iy \in \mathbb{Z}[i]$ is $\mathcal{N}(x + iy) = x^2 + y^2$.

Note that any odd integer $x + iy$ has an associated primary which can be obtained upon multiplication by a unit. The following theorem will now be proved:

Theorem 1 *An odd prime p congruent 5 modulo 8 has the representation, as a sum of two squares, of the form $p = (2X + 1)^2 + 4(2Y + 1)^2$, then in $\mathbb{Z}[i]$ it decomposes as*

$$p = ((2X + 1) + 2(2Y + 1)i)((2X + 1) - 2(2Y + 1)i) \ ,$$

and a primary factor is

$$\pi = ((2X+1) + 2(2Y+1)i)(-1)^{X-1} \ .$$

PROOF Since p can be written as the sum of two squares $p = (2X+1)^2 + 4y^2$, the first part of the lemma is proved by showing that y is odd. Taking p modulo 8 we have

$$p \bmod 8 = 5 = 4X(X+1) + 1 + 4y^2 = 1 + 4y^2 \Rightarrow 4y^2 = 4 \bmod 8 \Rightarrow y^2 = 1 \bmod 2 \ ,$$

which implies $y = 1 \bmod 2$.
The prime factor π of p in $\mathbb{Z}[i]$ is primary if it is congruent 1 modulo $-2+2i$. Imposing this condition, with u a unit, and considering that $4 = 0 \bmod (-2+2i)$, we have

$$1 = ((2X+1) + 2i(2Y+1))u \bmod (-2+2i) = u(2X+3) \bmod (-2+2i) \ ,$$

because $2i = 2 \bmod (-2+2i)$. We distinguish two cases:

1. If X is even then u must satisfy the condition $3u = 1 \bmod (-2+2i)$, which forces $u = -1$, that is $u = (-1)^{X-1}$.
2. If X is odd then u must satisfy the condition $5u = 1 \bmod (-2+2i)$, which forces $u = 1$, that is, again, $u = (-1)^{X-1}$.

This concludes the proof.

□

Let $\pi \in \mathbb{Z}[i]$ be an irreducible of odd norm, and $\pi \nmid \alpha$. There exists a unique integer j, [16, p.122], such that

$$\alpha^{\frac{\mathcal{N}(\pi)-1}{4}} = i^j \bmod \pi \ .$$

This property is used to define a quartic residue symbol as

$$\left[\frac{\alpha}{\pi}\right]_4 = \begin{cases} i^j & \text{if } \pi \nmid \alpha \\ 0 & \text{otherwise} \end{cases} \ .$$

Let $\nu = a + ib$ be a primary odd number, then a Jacobi-like symbol for quartic residues, written as $\left[\frac{\beta}{\nu}\right]_4$ and called the Gauss-Jacobi symbol, is defined multiplicatively, similarly to the Jacobi symbol in the quadratic case. It satisfies the following properties [16, 20] that allow us to evaluate the symbol without knowing the factorization of the arguments:

1. $\left[\frac{\alpha+\mu\nu}{\nu}\right]_4 = \left[\frac{\alpha}{\nu}\right]_4$,
2. $\left[\frac{\alpha\beta}{\nu}\right]_4 = \left[\frac{\alpha}{\nu}\right]_4 \left[\frac{\beta}{\nu}\right]_4$,
3. $\left[\frac{i}{\nu}\right]_4 = i^{-\frac{a-1}{2}}$ and thus $\left[\frac{-1}{\nu}\right]_4 = (-1)^{\frac{a-1}{2}}$,

4. $\left[\frac{1+i}{\nu}\right]_4 = i^{\frac{a-1-b-b^2}{4}}$ and thus $\left[\frac{2}{\nu}\right]_4 = i^{\frac{-b}{2}}$,

5. If $\omega = c + di$ is a primary number of odd norm, its real part c is odd, then either c or $-c$ is congruent 1 modulo 4; it follows that the real part of ω or $-\omega$ is congruent 1 modulo 4. Let $\alpha = u + vi$ and $\beta = t + wi$ have odd norm, with the real part congruent 1 modulo 4; the reciprocity law takes the Jacobi-Kaplan form

$$\left[\frac{\alpha}{\beta}\right]_4 \left[\frac{\beta}{\alpha}\right]_4^{-1} = (-1)^{\frac{v\cdot w}{4}} \ .$$

The main theorem of this section provides the means to identify the four square roots of a quadratic residue in $\mathbb{Z}[i]$ using only two bits and without unveiling the factorization of N or ν.
Proceeding as previously in the definition of ψ_1 and ψ_2, given π_1, π_2 relatively prime integers in $\mathbb{Z}[i]$, we can find ξ_1, ξ_2 such that $\xi_1 + \xi_2 = 1$, $\xi_1 = \mu_2\pi_2$ and $\xi_2 = \mu_1\pi_1$ for some $\mu_1, \mu_2 \in \mathbb{Z}[i]$, and set $\xi = \xi_1 - \xi_2$, which turns out to be a square root of 1 modulo $\nu = \pi_1\pi_2$, i.e. $\xi^2 = 1 \bmod \nu$.

Theorem 2 *Let $\nu = \pi_1\pi_2$ be the product of two primary primes having norms congruent 5 modulo 8. A root α among the four square roots $\{\gamma, -\gamma, \gamma\xi, -\gamma\xi\}$ of a quadratic residue $\beta = \alpha^2 \bmod \nu$ can be uniquely identified with two bits b_0 and b_1 defined as:*

$$b_0 = \begin{cases} 1 & \text{if} \quad \Re(\alpha) > 0 \\ 0 & \text{if} \quad \Re(\alpha) < 0 \end{cases} \ ,$$

(use $\Im(\alpha)$ if $\Re(\alpha) = 0$);

$$b_1 = \begin{cases} 1 & \text{if} \quad \left[\frac{\alpha}{\nu}\right]_4 \in \{1, i\} \\ 0 & \text{if} \quad \left[\frac{\alpha}{\nu}\right]_4 \in \{-1, -i\} \end{cases} \ .$$

PROOF. With the given choice of b_0, the parameter b_1 must discriminate α from $\alpha\xi$ or $-\alpha\xi$. Due to the multiplicative property of the Gauss-Jacobi symbol, this is tantamount to showing that $\left[\frac{\xi}{\nu}\right]_4 = \left[\frac{-\xi}{\nu}\right]_4 = -1$. Indeed we have

$$\left[\frac{\xi}{\nu}\right]_4 = \left[\frac{\xi}{\pi_1}\right]_4 \left[\frac{\xi}{\pi_2}\right]_4 = \left[\frac{\xi_1 - \xi_2}{\pi_1}\right]_4 \left[\frac{\xi_1 - \xi_2}{\pi_2}\right]_4 = \left[\frac{\xi_1}{\pi_1}\right]_4 \left[\frac{-\xi_2}{\pi_2}\right]_4 \ .$$

But $\xi_1 = 1 - \xi_2$ and conversely $\xi_2 = 1 - \xi_1$, so we obtain the expression

$$\left[\frac{\xi}{\nu}\right]_4 = \left[\frac{1 - \xi_2}{\pi_1}\right]_4 \left[\frac{-(1 - \xi_1)}{\pi_2}\right]_4 = \left[\frac{1}{\pi_1}\right]_4 \left[\frac{-1}{\pi_2}\right]_4 = -1 \ .$$

This conclusion follows because, by Theorem 1, π_2 is of the form $((2X+1) + 2(2Y+1)i)(-1)^{X-1}$, which implies

$$\left[\frac{-1}{\pi_2}\right]_4 = (-1)^{\frac{(2X+1)(-1)^{X-1}-1}{2}} = -1 \ ,$$

since the exponent is always odd, whatever be the parity of X.
In the same way $\left[\frac{-\xi}{\nu}\right]_4 = -1$ by exchanging the roles of π_1 and π_2.
In summary, $\left[\frac{\alpha}{\nu}\right]_4 = -\left[\frac{\alpha\xi}{\nu}\right]_4 = -\left[\frac{-\alpha\xi}{\nu}\right]_4$, then $b_1 \in \{0,1\}$ distinguishes between the two roots with the same b_0.

□

Remark 3. Let N be equal to the norm of ν, then a representation of the elements of the finite ring $\mathfrak{Z}_\nu = \mathbb{Z}[i]/\nu\mathbb{Z}[i]$, which is isomorphic to $\mathbb{Z}_N$, may consist of the same elements of $\mathbb{Z}_N$. A more "natural" representation of $\mathfrak{Z}_\nu$ consists of N elements of $\mathbb{Z}[i]$, which have minimum Euclidean norm and are not congruent to one another modulo ν. The two representations are perfectly equivalent, the use of one or the other only depending on the simplicity of computations and arithmetic operations in $\mathbb{Z}[i]/\nu\mathbb{Z}[i]$.

Let $N = pq$ be decomposed in $\mathbb{Z}[i]$ as a product $\nu\bar{\nu}$, where $\nu = \pi_1\pi_2$ is the product of an irreducible factor of p and an irreducible factor of q. Noting that ν and $\bar{\nu}$ are relatively prime, any number f of $\mathbb{Z}_N$ is uniquely identified by the pair $[f_1, f_2]$ obtained by taking the remainders modulo ν and modulo $\bar{\nu}$, i.e. $f_1 = f \bmod \nu$, $f_2 = f \bmod \bar{\nu}$, and f_2 is easily seen to be the complex conjugate $\bar{f}_1$ of f_1. The value f is recovered from the pair $[f_1, \bar{f}_1]$, by using the Chinese remainder theorem

$$f = f_1\zeta_1 + \bar{f}_1\zeta_2 \mod N \ , \tag{9}$$

where $\zeta_1 = \mu_1\bar{\nu} \bmod N$, and $\zeta_2 = \mu_2\nu \bmod N$, are the complex counterparts of ψ_1 and ψ_2, with μ_1 and μ_2 computed by means of the generalized Euclidean algorithm. It is pointed out, as a consequence of equation (9), that a quadratic residue m modulo N is also a quadratic residue modulo ν, and a square root A of m modulo N corresponds to a square root α of m modulo ν. Considering ψ, as defined in (4), we have that $-A$ corresponds to $-\alpha$, $A\psi$ corresponds to $\alpha\xi$, and $-A\psi$ corresponds to $-\alpha\xi$ because $\xi = \psi \bmod \nu$. This last identity is straightforwardly proved, by observing that

$$1 = \psi_1 + \psi_2 = \lambda_2 q + \lambda_1 p = \lambda_2\pi_2\bar{\pi}_2 + \lambda_1\pi_1\bar{\pi}_1$$

in $\mathbb{Z}[i]$, thus, taking the remainder modulo ν, we have

$$1 = (\lambda_2\bar{\pi}_2)\pi_2 + (\lambda_1\bar{\pi}_1)\pi_1 \bmod \nu = \xi_1 + \xi_2 \bmod \nu \ ,$$

due to the definition of ξ_1 and ξ_2, and finally $\xi_1 = \psi_1 \bmod \nu$ and $\xi_2 = \psi_2 \bmod \nu$, by the Chinese remainder theorem.

A Rabin scheme working with primes p and q congruent 5 modulo 8 can then be defined, by considering the decomposition $N = \nu\bar{\nu}$ with $\nu = \pi_1\pi_2$ being the product of two primary factors of p and q respectively.

Public-key: $[\nu]$.

Message: m.

Encrypted message $[C, b_0, b_1]$, where

$$C = m^2 \bmod N \quad , \quad b_0 = m \bmod 2 \quad , \text{ and } \quad b_1 = \begin{cases} 1 & \text{if } \left[\frac{m}{\nu}\right]_4 \in \{1, i\} \\ 0 & \text{if } \left[\frac{m}{\nu}\right]_4 \in \{-1, -i\} \end{cases} .$$

Decryption stage :

- compute, as in (3), the four roots of C modulo N, written as positive numbers,
- take the two roots having the same parity specified by b_0, say z_1 and z_2,
- compute the quartic residues

$$\left[\frac{z_1}{\nu}\right]_4 \qquad \left[\frac{z_2}{\nu}\right]_4 ,$$

and take the root corresponding to b_1.

4.1.1 Semantic security of the Rabin scheme with $p = q = 5 \bmod 8$

In [29] semantic security is considered for pairs of Blum primes by means of the so-called Rabin-Paillier's scheme. It is shown that the same scheme works equally well for pairs of primes $p = q = 5 \bmod 8$, provided that quartic residuosity is used. Rabin-Paillier's encryption scheme is recalled and adapted as follows.

- **Secret key:** Two prime numbers $p = q = 5 \bmod 8$ are factored in $\mathbb{Z}[i]$ as $p = \pi_1 \bar{\pi}_1$ and $q = \pi_2 \bar{\pi}_2$, π_1 and π_2 primary.
- **Public key:** $\nu = \pi_1 \pi_2$, e, where e is a prime $\frac{|n|}{2} < |e| < |n|$ with $n = \nu \bar{\nu}$, and $|n|$ being the bit-length of n.
- **Plaintext:** $m \in \mathbb{Z}_n$
- **Ciphertext:**

$$c = r^{2e} + mn \bmod n^2 \tag{10}$$

where $r \in \mathbb{Z}_n$ is randomly chosen such that $\left[\frac{r}{\nu}\right]_4 = 1$ and $r > \frac{n}{2}$.

- **Decryption:** Let $E = c^d \bmod n$, where $ed = 1 \bmod \phi(n)$, then it is immediate to see that

$$E = r^2 \bmod n \ .$$

We can solve the quadratic equation $x^2 = E \bmod n$, and find $r > \frac{n}{2}$ uniquely satisfying $\left[\frac{r}{\nu}\right]_4 = 1$. Finally, substituting into (10), we obtain m.

Remark 4. It should be noted that Rabin-Paillier's encryption scheme exploits, as does the Rabin scheme, the difficulty of computing the roots of quadratic equations in residue rings, but is otherwise a completely different algorithm.
Further, it is noted that semantic security is achieved under proper assumptions and by doubling the number of bits of the encrypted message. This extra cost seems to be unavoidable [19].

4.2 General scenario: any pair of primes

In principle, root identification in the case of pairs of primes p and q of the type $4k+1$, which are congruent modulo a suitable power 2^t, may be achieved by considering residuosity of higher order and cyclotomic fields $\mathbb{Q}(\zeta_{2^t})$ as shown in equation (8). The plan is to consider residuosity of order 2^t so that -1 is non-residue modulo prime factors of p and q in $\mathbb{Q}(\zeta_{2^t})$, and evaluate the 2^t-th residue modulo a factor ν of N in $\mathbb{Q}(\zeta_{2^t})$ using some form of reciprocity that allows a reduction via the Euclidean algorithm, operations that do not disclose the factorization of N. However, a limit upon this plan is that its extension to residuosity of higher order is straightforward only up to $\mathbb{Q}(\zeta_{32})$ because these fields are Euclidean [17]. The next field, $\mathbb{Q}(\zeta_{64})$, has class number 17, thus is certainly not Euclidean, hence a reduction via the Euclidean algorithm is not possible. Also, integer division with remainder may not be easy to perform in the fields $\mathbb{Q}(\zeta_{2^t})$, $t \geq 4$. It is known that for Gaussian integers $\mathbb{Z}[i]$, i.e. $t = 2$, the division may be performed by *rounding* the entries of the quotient of integers $v = \frac{v_0+v_1 i}{\nu} = (a_0; a_1) \in \mathbb{Q}^2$ to their nearest integers, $a'_0 + a'_1 i = (\lfloor a_0 + \frac{1}{2} \rfloor; \lfloor a_1 + \frac{1}{2} \rfloor) \in \mathbb{Z}^2$. The remainder of minimum norm is obtained as $r_0 + r_1 i = (v_0 + v_1 i) - \nu \cdot (a_0 + a_1 i)$.
It is also known that the 1-step norm-Euclidean algorithm for $\mathbb{Z}[\zeta_8]$, i.e. $t = 3$, devised by Eisenstein [7], is implicitly defined by *rounding*, and [22, Sec. 4.1] includes an explicit proof.
In point of fact, the use of residuosity appears in practice to be not convenient, perhaps impossible, even for primes of the form $2^t(2k+1)+1$, $t \geq 3$. Further, it does not work for pairs of primes with different residues modulo 2^t. In the search for different solutions, the next section proposes a scheme that allows the roots in Rabin algorithm to be identified, that works for every pair of primes.

4.2.1 Group isomorphisms

In this section, a method is described that works for any pair of primes, which may have acceptable complexity and be of practical interest, although it requires a one-way function that might be weaker than factoring, and entails communicating more bits than the theoretical lower bound of 2. The following approach relies on the difficulty of computing discrete logarithms.
Given N, let $P = \mu N + 1$ be a prime (the smallest prime), that certainly exists by Dirichlet's theorem [1], that is congruent 1 modulo N. Let g be a primitive element generating the multiplicative group $\mathbb{Z}_P^*$.

Define $g_1 = g^\mu$ and $g_2 = g^{\mu(\psi_1 - \psi_2)}$, and as usual let m denote the message.

Public key: $[N, P, g_1, g_2]$.

Encryption stage: $[C, b_0, d_1, d_2, p_1, p_2]$, where $C = m^2 \bmod N$, $b_0 = m \bmod 2$, p_1 is a position in the binary expansion of $g_1^m \bmod P$, whose bit d_1 is different from the bit in the corresponding position of the binary expansion of $g_2^m \bmod P$, and p_2 is a position in the binary expansion of

$g_1^m \bmod P$, whose bit d_2 is different from the bit in the corresponding position of the binary expansion of $g_2^{-m} \bmod P$.

Decryption stage :

- compute, as in (3), the four roots, written as positive numbers,
- take the two roots having the same parity specified by b_0, say z_1 and z_2,
- compute $A = g_1^{z_1} \bmod P$ and $B = g_1^{z_2} \bmod P$
- between z_1 and z_2, the root is selected that has the correct bits d_1 and d_2 in both the given positions p_1 and p_2 of the binary expansion of A or B.

The algorithm is justified by the following Lemma. Notice that g_2^{-m} must also be considered because, using notations of Lemma 1, it is necessary to distinguish e.g. x_1 from x_2 or x_3, but it is not known which of the two, a priori.

Lemma 6 *The power $g_0 = g^\mu$ generates a cyclic group of order N in $\mathbb{Z}_P^*$, thus the correspondence $x \leftrightarrow g_0^x$ establishes an isomorphism between a multiplicative subgroup of $\mathbb{Z}_P^*$ and the additive group of $\mathbb{Z}_N$. Let z_0 denote any of the four roots z_1, z_2, z_3, z_4 of $x^2 = C \bmod N$, $\left(\frac{C}{p}\right) = \left(\frac{C}{q}\right) = 1$; these four roots, in the order*

$$\{z_0,\ -z_0,\ z_0(\psi_1 - \psi_2),\ -z_0(\psi_1 - \psi_2)\}\ ,$$

are in a one-to-one correspondence with the ordered four powers of g_0 computed modulo P

$$\{g_0^{z_0},\ g_0^{-z_0},\ g_0^{z_0(\psi_1-\psi_2)},\ g_0^{-z_0(\psi_1-\psi_2)}\}\ ,$$

and different values of z_0 simply yield a re-ordering of this set.

PROOF. The first part is due to the choice of P: the group generated by g_0 has order N, thus the isomorphism follows immediately. The second part is a consequence of Section 2.1.

□

The price to pay is the costly arithmetic in $\mathbb{Z}_P$, and the equivalence of the security of the Rabin cryptosystem with the hardness of factoring is now conditioned by the complexity of computing the discrete logarithm in $\mathbb{Z}_P$.

Remark 5. In line with the above solution, the following more general approach is possible: choose a one-way function $\mathfrak{d}$ (exponentiation with base g_1 above) defined from $\mathbb{Z}_N$ into a group $\mathfrak{G}$ of the same order, and build from it a function $\mathfrak{d}_1$(exponentiation with base g_2 above) such that $\mathfrak{d}_1(x_1) = \mathfrak{d}(x_2)$, with x_1 and x_2 as defined in Lemma 1. The public key contains the two functions $\mathfrak{d}$ and $\mathfrak{d}_1$. At the encryption stage, both are evaluated at the same argument, the message m, and the minimum information necessary to distinguish their values is delivered together with the encrypted message. The true limitation of this scheme is that $\mathfrak{d}$ must be a one-way function, otherwise two square roots that allow us to factor N can be recovered, as shown earlier in dealing with residuosity.

Remark 6. Some variants of this method that may be of practical interest are:

1. In the scheme of section 4.2.1, instead of considering the parity bit of the plain message, a bit indicating whether the message is greater or smaller than $\frac{N}{2}$ does the job; note that this bit does not reveal the parity of the message.

2. In the scheme of section 4.2.1, instead of using a parity bit or the variant proposed in point 1, a further pair d_3 and p_3 (defined similarly to d_1 and p_1 considering the power g_1^{-m}) is sent at some extra cost, but no information about the plain message is revealed.

5 The Rabin signature

In the introduction, it was said that a Rabin signature of a message m may consist of a pair $[n, S]$; however, if $x^2 = m \bmod N$ has no solution, this signature cannot be directly generated. To overcome this obstruction, a random pad U was proposed [25]; attempts are repeated until $x^2 = mU \bmod N$ is solvable, and the signature is the triple (m, U, S), [25]. A verifier compares $mU \bmod N$ with S^2 and accepts the signature as valid when these two numbers are equal.
This section presents a modified version of this scheme, in which no attempts are needed to derive U. Now, the quadratic equation $x^2 = m \bmod N$ is solvable if and only if m is a quadratic residue modulo N, that is m is a quadratic residue modulo p and modulo q. When m is not a quadratic residue, it is shown below how to exploit the Jacobi symbol to compute a suitable pad and obtain quadratic residues modulo p and q. Let
$f_1 = \frac{m_1}{2}\left[1 - \left(\frac{m_1}{p}\right)\right] + \frac{1}{2}\left[1 + \left(\frac{m_1}{p}\right)\right]$, $f_2 = \frac{m_2}{2}\left[1 - \left(\frac{m_2}{q}\right)\right] + \frac{1}{2}\left[1 + \left(\frac{m_2}{q}\right)\right]$.
Writing $m = m_1\psi_1 + m_2\psi_2$, the equation

$$x^2 = (m_1\psi_1 + m_2\psi_2)(f_1\psi_1 + f_2\psi_2) = m_1 f_1 \psi_1 + m_2 f_2 \psi_2$$

is always solvable modulo N, because $m_1 f_1$ and $m_2 f_2$ are clearly quadratic residues modulo p and modulo q, respectively, since $\left(\frac{m_1}{p}\right) = \left(\frac{f_1}{p}\right)$, $\left(\frac{m_2}{q}\right) = \left(\frac{f_2}{q}\right)$, so that

$$\left(\frac{m_1 f_1}{p}\right) = \left(\frac{m_1}{p}\right)\left(\frac{f_1}{p}\right) = 1\ ,\ \left(\frac{m_2 f_2}{q}\right) = \left(\frac{m_2}{q}\right)\left(\frac{f_2}{q}\right) = 1\ .$$

Note that if p and q are Blum primes, it is possible to choose $f_1 = \left(\frac{m_1}{p}\right)$ and $f_2 = \left(\frac{m_2}{q}\right)$. The following procedure may be described:

Public-key: N

Signed message: $[U, m, S]$, where $U = R^2\,[f_1\psi_1 + f_2\psi_2] \bmod N$ is the padding factor, with R a random number, and S is any solution of the equation $x^2 = mU \bmod N$. R is needed to avoid knowledge of U enabling N to be easily factored.

Verification: compute $mU \bmod N$ and $S^2 \bmod N$; the signature is valid if and only if these two numbers are equal.

This signature scheme has several interesting features:

1. signature is possible using any pair of primes, and thus it could for example be used with the modulo of any RSA public key;

2. different signatures of the same document are different;

3. the verification only requires two multiplications, therefore it is fast enough to be used in authentication protocols.

5.1 Forgery attacks

Schemes of this type are, however, vulnerable to forgery attacks: it is relatively easy to compute $S^2 \bmod N$, choose any message m', compute $U' = S^2 m'^{-1} \bmod N$, and forge the signature as (m', U', s) without knowing the factorization of N. In some variants, a hash $H(m)$ is used instead of m and S is a solution of $x^2 = H(mU) \bmod N$, but this does not help against the above forgery attack. The following variant aims at countering this vulnerability.

Public-key: N

Signed message: $[m, UK^2 \bmod N, SK^3 \bmod N, K^4 \bmod N]$, where U is the padding factor, K a random number, and S is any solution of the equation $x^2 = mU \bmod N$.

Verification: compute $(SK^3)^2 \bmod N$ and $mUK^2K^4 \bmod N$; the signature is valid if and only if these two numbers are equal.

Note that U, K and S are not known. Forgery would be possible if K were known, but to know K one has to solve an equation of degree at least 2. To verify the signature only two multiplications and one square are needed.
Note that there is another signature scheme relying on the difficulty of finding square roots, the Rabin-Williams signature (cf. [12]), which avoids the forgery vulnerability. While that scheme requires the use of two primes, respectively congruent to 3 and 7 modulo 8, the two variants above do not need this condition. Moreover, in the Rabin-Williams scheme, a message cannot be signed twice in two different ways, otherwise the factorization of N might be exposed. In the above schemes, using a deterministic pad as above allows different signatures of the same message.
For more on forgery and blindness on Rabin signatures, please refer also to [8].

6 Conclusions and Remarks

A few comments follows on Rabin schemes in general, after having mainly dwelt on deterministic aspects and identification problems.
In principle, the Rabin scheme is very efficient because only one square is required for encryption; furthermore, it is provably as secure as factoring. Nevertheless, it is well known [4, 15] that it presents some drawbacks, mainly due to the four-to-one mapping, that may discourage its use to conceal the content of a message. These are:

- root identification requires the delivery of additional information, which may increase computational costs;

- many proposed root identification methods, based on the message semantics, have a probabilistic character and cannot be used in some circumstances;
- the delivery of two bits together with the encrypted message exposes the process to active attacks by maliciously modifying these bits. For example, suppose an attacker A sends an encrypted message to B asking that the decrypted message be delivered to a third party C (a friend of A). If in the encrypted message the bit that identifies the root, between the two roots of the same parity, had been deliberately changed, A can get a root from C that, combined with the original message, enables the Rabin public-key to be factored. Even our Variant II is not immune to this kind of active attack.

In conclusion, the Rabin scheme may suffer from some drawbacks when used to conceal a message, whereas it seems effective when applied to generate an electronic signature or as a hash function. However, these observations do not exclude the practical use of the Rabin scheme (as is actually done in some standardized protocols), when other properties, like integrity and authenticity, need to be safeguarded, along with message secrecy, in a public-encryption protocol.

7 Acknowledgments

Some of this work was done while the first author was Visiting Professor with the University of Trento, funded by CIRM, and he would like to thank the Department of Mathematics for the friendly and fruitful atmosphere offered. The third author was supported by the Swiss National Science Foundation under grant No. 132256. We would also like to thank Steven Galbraith for his comments on a preliminary version of the paper and for pointing out some references.
Finally, we gratefully acknowledge the many suggestions and corrections offered by anonymous referees which have greatly improved the readability and quality of the paper.

References

[1] T.M. Apostol, *Introduction to Analytic Number Theory*, Springer, New York, 1976.

[2] E. Bach, J. Shallit, *Algorithmic Number Theory*, MIT, Cambridge Mass., 1996.

[3] D.J. Bernstein, Proving tight security for Rabin-Williams signatures, EUROCRYPT 2008 (N. P. Smart, ed.), LNCS, vol. 4965, Springer, 2008, pp. 70–87.

[4] J.A. Buchmann, *Introduction to Cryptography*, Springer, New York, 1999.

[5] D.G. Cantor, H. Zassenhaus, A new Algorithm for Factoring Polynomials over Finite Fields, *Math. Comp.*, Vol. 36, N. 154, April 1981, pp.587-592.

[6] R. Dedekind, Schreiben an Herrn Borchardt, *J. Reine Angew. Math.*, 83, 1877, pp.265-292.

[7] G. Eisenstein, Über einige allgemeine Eigenschaften der Gleichung, von welcher die Theilung der ganzen Lemniscate abhängt, nebst Anwendungen derselben auf die Zahlentheorie, *J. Reine Angew. Math.*, 39 (1850), 224-274; 275-287.

[8] M. Elia, D. Schipani, On the Rabin signature, *J. Discrete Math. Sci. Cryptogr.*, Vol. 16, no.6, (2013), pp.367-378.

[9] M. Elia, D. Schipani, Improvements on the Cantor-Zassenhaus Factorization Algorithm, to appear in *Math. Bohem.*

[10] D.M. Freeman, O. Goldreich, E. Kiltz, A. Rosen, G. Segev, More Constructions of Lossy and Correlation-Secure Trapdoor Functions, PKC 2010, Springer LNCS 6056 (2010), pp.279-295.

[11] A. Fröhlich, M.J. Taylor, *Algebraic Number Theory*, Cambridge Univ. Press, 1994.

[12] S. Galbraith, *The Mathematics of Public Key Cryptography*, Cambridge Univ. Press, 2012.

[13] E. Grosswald, *Topics from the Theory of Numbers*, Birkhäuser, Basel, 2009.

[14] G.H. Hardy, E.M. Wright, *An Introduction to the Theory of Numbers*, Oxford at the Clarendon Press, 1971.

[15] J. Hoffstein, J. Pipher, J.H. Silverman, *An introduction to mathematical cryptography*, Springer, New York, 2008.

[16] K. Ireland, M. Rosen, *A Classical Introduction to Modern Number Theory*, Springer, New York, 1998.

[17] N. Kaiblinger, Cyclotomic rings with simple Euclidean algorithm, *JP J. Algebra Number Theory Appl.*, 23, no. 1, 2011, pp.61-76.

[18] K. Kurosawa, T. Itoh, and M. Takeuchi, Public Key Cryptosystem Using a Reciprocal Number with the same Intractability as Factoring a Large Number, *CRYPTOLOGIA*, vol. XII, pp. 225-233, 1988.

[19] K. Kurosawa, T. Takagi, One-Wayness Equivalent to General Factoring, *IEEE Trans. on Inform. Theory*, vol. 55, No.9, September 2009, pp. 4249-4262.

[20] F. Lemmermeyer, *Reciprocity Laws*, Springer, New York, 2000.

[21] A.J. Menezes, P.C. van Oorschot, S.A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, Boca Raton, 1997.

[22] C. Monico, M. Elia, On the Representation of Primes in $\mathbb{Q}(\sqrt{2})$ as Sums of Squares, *JP J. Algebra Number Theory Appl.*, 8, no. 1, 2007, pp.121-133.

[23] Paillier P., Public-Key Cryptosystems Based on Composite Degree Residuosity Classes, EUROCRYPT, Springer. (1999), pp. 223238.

[24] Paillier P., Pointcheval D., Efficient Public-Key Cryptosystems Provably Secure Against Active Adversaries, Advances in Cryptology - ASIACRYPT99, *Lecture Notes in Computer Science*, Volume 1716, 1999, pp 165-179

[25] J. Pieprzyk, T. Hardjono, J. Seberry, *Fundamentals of Computer Security*, Springer, New York, 2003.

[26] M. Rabin, Digitalized signature as intractable as factorization,
Technical Report MIT/LCS/TR-212, MIT Laboratory for Computer Science, January 1978.

[27] H. Rademacher, E. Grosswald, *Dedekind Sums*, MAA, New York, 1972.

[28] B. Schneier, *Applied cryptography*, Wiley, 1996.

[29] T. Takagi, S. Naito, Extension of Rabin Cryptosystem to Eisenstein and Gauss Fields, *IEICE Trans. Fundamentals*, Vol. E80-A, No. 4, April 1997.

[30] J. von zur Gathen, J. Gerhard, *Modern Computer Algebra*, Cambridge Univ. Press, 1999.

[31] H.C. Williams, A modification of the RSA public-key encryption procedure, *IEEE Trans. on Inform. Th.*, IT-26(6), November 1980, pp.726-729.